IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method for preserving confidentiality of an electronic mail from a sender to a recipient, comprising:
authenticating identity information of the recipient;
restricting the recipient's ability to manipulate contents of the electronic mail based on a confidentiality level established by the sender;
encrypting the electronic mail, at the recipient, with the authenticated identity information if the recipient attempts to store the electronic mail to a local storage; and
decrypting the electronic mail, at the recipient, if the recipient attempts to retrieve the electronic
mail from the local storage.

2. (Original) The method according to claim 1, wherein the identity information is a system password.

3. (Original) The method according to claim 1, the method further comprising:
prompting a user of the recipient to supply the identity information;
decrypting the electronic mail with the identity information supplied by the user.

4. (Original) The method according to claim 1, the method further comprising:
asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold.

5. (Original) The method according to claim 4, wherein the control signal is a confidentiality-level-dependent control signal.

6. (Currently Amended) An electronic mail confidentiality preserver of [[an]] a recipient email client, comprising:

an input-processing engine to limit abilities of a user of the recipient email client to manipulate contents of an electronic mail received by the recipient email client based on a confidentiality level; and

an encryption/decryption engine, coupled to the input-processing engine, to encrypt the electronic mail with authenticated identity information if the recipient attempts to store the electronic mail to a local storage.

7. (Original) The electronic mail confidentiality preserver according to claim 6, the input-processing engine further asserts a first control signal to disable options that are originally supported by the email client if the confidentiality level satisfies a predefined confidentiality threshold.

8. (Original) The electronic mail confidentiality preserver according to claim 7, wherein the first control signal is a confidentiality-level-dependent control signal.

9. (Original) The electronic mail confidentiality preserver according to claim 6, the input-processing engine further asserts a second control signal to invoke the encryption/decryption engine in response to the user's access.

10. (Original) The electronic mail confidentiality preserver according to claim 6, the encryption/decryption engine further

prompts the user for identity information;

if the user's access to the local storage is to store the electronic mail, encrypts the electronic mail with the identity information; and

if the user's access to the local storage is to retrieve the electronic mail, decrypts the electronic mail with the identity information.

11. (Currently Amended) A recipient electronic mail client, comprising:

a user interface;

a communication engine;

a local storage;

and an electronic mail confidentiality preserver, coupled to the user interface, coupled to the communication engine and coupled to the local storage, wherein the electronic mail confidentiality preserver further comprises:

an input-processing engine to limit abilities of a user of the recipient email client to manipulate contents of an electronic mail received by the recipient email client based on a user-selected confidentiality level; and

an encryption/decryption engine, coupled to the input-processing engine, to encrypt the electronic mail with authenticated identity information if the recipient attempts to store the electronic mail to a local storage.

12. (Original) The electronic mail client according to claim 11, wherein the user interface further comprises:

a first set of confidentiality levels for the user to select from; and

a second set of options to manipulate the electronic mail for the user to select from.

13. (Original) The electronic mail client according to claim 12, wherein the electronic mail confidentiality preserver further asserts a first control signal to the user interface to disable selected options from the second set of options if the confidentiality level satisfies a predefined confidentiality threshold.

14. (Original) The electronic mail client according to claim 13, wherein the first control signal is a confidentiality-level-dependent control signal.

15. (Original) The electronic mail client according to claim 12, the input-processing engine further asserts a second control signal to invoke the encryption/decryption engine in response to the user's access.

16. (Original) The electronic mail client according to claim 12, the encryption/decryption

engine further

prompts the user for identity information;

if the user's access to the local storage is to store the electronic mail, encrypts the electronic mail with the identity information; and

if the user's access to the local storage is to retrieve the electronic mail, decrypts the electronic mail with the identity information.

17. (Currently Amended) A machine readable medium including a plurality of instructions readable therefrom, the instructions, when executed by a computer system, cause the computer system to perform operations comprising:

authenticating identity information of a recipient of an electronic mail;

restricting the recipient's ability to manipulate contents of the electronic mail based on a confidentiality level established by a sender of the electronic mail;

encrypting the electronic mail, at the recipient, with the authenticated identity information if the recipient attempts to store the electronic mail to a local storage; and

decrypting the electronic mail, at the recipient, if the recipient attempts to retrieve the electronic mail from the local storage.

18. (Original) The machine readable medium according to claim 17, wherein the identity information is a system password.

19. (Original) The machine readable medium according to claim 17, the instructions further comprising:

prompting a user of the recipient to supply the identity information;

decrypting the electronic mail with the identity information supplied by the user.

20. (Original) The machine readable medium according to claim 17, the instructions further comprising:

asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold.

21. (Original) The machine readable medium according to claim 20, wherein the control signal is a confidentiality-level-dependent control signal.